Final remarks on local discriminants

Chandan Singh Dalawat
Harish-Chandra Research Institute
Chhatnag Road, Jhunsi, Allahabad 211019, India
dalawat@gmail.com

Abstract. We show how the ramification filtration on the maximal elementary abelian p-extension (p prime) on a local number field of residual characteristic p can be derived using only Kummer theory and a certain orthogonality relation for the Kummer pairing, even in the absence of a primitive p-th root of 1 ; the case of other local fields was treated earlier. In all cases, we compute the contribution of cyclic extensions to Serre's degree-p mass formula.

1. Introduction. — Let p be a prime number, and K a local number field or a local function field of residual characteristic p, so that K is a finite extension of $\mathbf{Q}_p$ or of $\mathbf{F}_p(\!(\pi)\!)$, where π is transcendental. Let M be the maximal elementary abelian p-extension of K, and $\mathrm{G} = \mathrm{Gal}(\mathrm{M}|\mathrm{K})$. The profinite group G comes with a natural filtration $(\mathrm{G}^u)_{u\in[-1,+\infty[}$ (in the upper numbering). Local class field theory provides an isomorphism $\mathrm{K}^\times/\mathrm{K}^{\times p} \to \mathrm{G}$ preserving the filtrations and thereby determines $(\mathrm{G}^u)_u$.

But a more elementary derivation is possible. Namely, when K is a local function field, a certain orthogonality relation for the Artin-Schreier pairing allows us to determine the filtration $(\mathrm{G}^u)_u$ in terms of the filtration on $\mathrm{K}/\wp(\mathrm{K})$ [**3**], §5. Also, when K is a local number field containing a primitive p-th root ζ of 1, the analogous orthogonality relation for the Kummer pairing allows us to determine $(\mathrm{G}^u)_u$ in terms of the filtration on $\mathrm{K}^\times/\mathrm{K}^{\times p}$ [**3**], §4.

The first purpose of this Note is to determine $(\mathrm{G}^u)_u$ when K is a local number field but $\zeta \notin \mathrm{K}$. The idea is to determine the filtered subspace $\mathrm{V} \subset \mathrm{K}(\zeta)^\times/\mathrm{K}(\zeta)^{\times p}$ corresponding to the exponent-p kummerian extension $\mathrm{M}(\zeta)|\mathrm{K}(\zeta)$, and then use the orthogonality relation for the Kummer pairing $\mathrm{G}\times\mathrm{V} \to {}_p\mu$ to deduce $(\mathrm{G}^u)_u$.

The subspace V is determined in §2 in a purely algebraic context. The filtration on V, the orthogonality relation, and the filtration $(\mathrm{G}^u)_u$ are

Keywords : Local fields, elementary abelian p-extensions, ramification filtration, discriminants, Serre's mass formula.

derived in §4. An overall summary is provided in §5 to bring out the analogy between the three cases.

We then compute (§6) the contribution of degree-p cyclic extensions to Serre's mass formula for separable degree-p extensions of K. It turns out that an extension of the ideas in §2 and §4 from $K(\zeta)|K$ to $K(\sqrt[p-1]{K^\times})|K$, inspired by the paper [**5**], also leads to an elementary proof of the said mass formula, based only on Kummer theory [**2**] or Artin-Schreier theory [**3**] and some purely algebraic ingredients. See [**4**].

2. Algebraic preliminaries. — We shall need some purely algberaic results which are often used in the proof of the local [**1**, p. 155] or the global [**6**, p. 110] Kronecker-Weber theorem. Our presentation is intrinsic, and shows the equivalence of the statements in these two sources.

Let p be a prime number and let F be a field in which p is invertible. We want to understand the degree-p cyclic extensions of F in terms of those of $K = F(\zeta)$, where ζ is a primitive p-th root of 1.

Let $E|F$ be a cyclic extension of degree p. The extension $E(\zeta)|K$ is also cyclic of degree p; it corresponds therefore ("Kummer theory") to an $\mathbf{F}_p$-line $D \subset K^\times/K^{\times p}$. The group $\Delta = \mathrm{Gal}(K|F)$ acts on the latter space. Let $\omega : \Delta \to \mathbf{F}_p^\times$ be the cyclotomic character giving the action of Δ on the p-th roots of 1, so that $\sigma(\zeta) = \zeta^{\omega(\sigma)}$ for every $\sigma \in \Delta$.

Sometimes we think of the target of ω as being the interval $[1, p[\subset \mathbf{Z}$. For p odd, $(\mathbf{Z}/p\mathbf{Z})^\times$ is often identified with the torsion subgroup of $\mathbf{Z}_p^\times$.

Lemma 1. — *The $\mathbf{F}_p$-line D is Δ-stable, and Δ acts on D via ω.*

Let $a \in K^\times$ be such that its image $\bar{a}$ modulo $K^{\times p}$ generates D, and x a p-root of a, so that $E(\zeta) = K(x)$. We have $\sigma(\bar{a}) = \overline{\sigma(a)}$ for every $\sigma \in \Delta$. We have to first show that $\sigma(\bar{a}) \in D$. Identify Δ with $\mathrm{Gal}(E(\zeta)|E)$. For every $\sigma \in \Delta$, we have

$$K(x) = F(\zeta, x) = F(\sigma(\zeta), \sigma(x)) = K(\sigma(x))$$

and $(\sigma(x))^p = \sigma(x^p) = \sigma(a)$ is in $K^\times$, so $\bar{a}$ and $\overline{\sigma(a)}$ belong to the same $\mathbf{F}_p$-line, namely D. Hence D is Δ-stable.

Let $\eta : \Delta \to \mathbf{F}_p^\times$ be the character through which Δ acts on D, so that, for a generator τ of Δ, we have $\tau(x) = bx^{\eta(\tau)}$ for some $b \in K^\times$. Let g be the generator $x \mapsto \zeta x$ of the group $\mathrm{Gal}(K(x)|K)$, so that $g(\zeta) = \zeta$. Hence $\tau(g(x)) = \tau(\zeta x) = \zeta^{\omega(\tau)} b x^{\eta(\tau)}$, on the one hand.

On the other hand, $g(\tau(x)) = g(bx^{\eta(\tau)}) = b\zeta^{\eta(\tau)} x^{\eta(\tau)}$. But $\tau g = g\tau$; comparing the two computations, we get $\eta = \omega$. Cf. [**1**, p. 155].

Conversely,

LEMMA 2. — *For every Δ-stable $\mathbf{F}_p$-line $\mathrm{D} \subset \mathrm{K}^\times/\mathrm{K}^{\times p}$ on which Δ acts via ω, there is a (unique) degree-p cyclic extension $\mathrm{E}|\mathrm{F}$ such that $\mathrm{K}(\sqrt[p]{\mathrm{D}}) = \mathrm{E}(\zeta)$.*

Keep the notation of lemma 1. Notice first that the extension $\mathrm{K}(x)$ is galoisian over F, for it contains, for every $\sigma \in \Delta$, a p-th root of $\sigma(a)$, namely $bx^{\omega(\sigma)}$, where $b \in \mathrm{K}^\times$ is such that $\sigma(a) = a^{\omega(\sigma)}b^p$. If $\mathrm{Gal}(\mathrm{K}(x)|\mathrm{F})$ is commutative (it would then have to be cyclic because the orders of G and Δ are relatively prime), the fixed field under the index-p subgroup would be the desired E.

Let us show that $\mathrm{Gal}(\mathrm{K}(x)|\mathrm{F})$ is indeed commutative. We have seen that $\tau(x) = bx^{\omega(\tau)}$ (for some $b \in \mathrm{K}^\times$) and $g(x) = \zeta x$ (for some $\zeta \in {}_p\mu$). Therefore $\tau g(x) = \tau(\zeta x) = \zeta^{\omega(\tau)} b x^{\omega(\tau)}$. On the other hand, $g\tau(x) = g(bx^{\omega(\tau)}) = b\zeta^{\omega(\tau)} x^{\omega(\tau)}$. So the extension $\mathrm{K}(x)|\mathrm{F}$ is abelian, as claimed.

COROLLARY 3. — *Let V be the ω-eigenspace for the action of Δ on $\mathrm{K}^\times/\mathrm{K}^{\times p}$. The map $\mathrm{E} \mapsto \mathrm{D}$ defined by $\mathrm{E}(\zeta) = \mathrm{K}(\sqrt[p]{\mathrm{D}})$ is a bijection of the set of degree-p cyclic extensions $\mathrm{E}|\mathrm{F}$ onto the set of $\mathbf{F}_p$-lines $\mathrm{D} \subset \mathrm{V}$.*

As usual, V can also be written as the image of a certain projector $\varepsilon \in \mathbf{F}_p[\Delta]$, when $\mathrm{K}^\times/\mathrm{K}^{\times p}$ is regarded as an $\mathbf{F}_p[\Delta]$-module. Indeed, let $\varepsilon = (1/m)\sum_{\sigma\in\Delta} \omega(\sigma^{-1})\sigma \in \mathbf{F}_p[\Delta]$, where m is the order of Δ, so that m divides $p-1$. It is easily verified that $\tau\varepsilon = \omega(\tau)\varepsilon$ for every $\tau \in \Delta$:

$$\begin{aligned}
\tau\varepsilon &= \frac{1}{m}\sum_{\sigma\in\Delta} \tau.\omega(\sigma^{-1})\sigma \\
&= \frac{1}{m}\sum_{\sigma\in\Delta} \omega(\sigma^{-1})\tau\sigma \\
&= \frac{\omega(\tau)}{m}\sum_{\sigma\in\Delta} \omega((\tau\sigma)^{-1})\tau\sigma \\
&= \frac{\omega(\tau)}{m} m\varepsilon = \omega(\tau)\varepsilon.
\end{aligned}$$

Upon multiplying both sides by $\omega(\tau^{-1})$ and summing over $\tau \in \Delta$, we get $\varepsilon\sum_{\tau\in\Delta} \omega(\tau^{-1})\tau = m\varepsilon$, or $\varepsilon.m\varepsilon = m\varepsilon$, and, as m is invertible in $\mathbf{F}_p$, we get $\varepsilon^2 = \varepsilon$, showing that ε is an idempotent. (It is clear that $\varepsilon(\bar{x}) = \bar{1}$ for every $x \in \mathrm{F}^\times$.)

In view of this, the preceding lemmas can be reformulated as follows, to bring out their equivalence with [**6**, p. 110].

LEMMA 4. — *For every degree-p cyclic extension* E|F*, there is a unique* $\mathbf{F}_p$*-line* $\mathrm{D} \subset \varepsilon(\mathrm{K}^\times/\mathrm{K}^{\times p})$ *such that* $\mathrm{E}(\zeta) = \mathrm{K}(\sqrt[p]{\mathrm{D}})$*. Conversely, for every* $\mathbf{F}_p$*-line* $\mathrm{D} \subset \varepsilon(\mathrm{K}^\times/\mathrm{K}^{\times p})$*, there is a unique degree-p cyclic extension* E|F *such that* $\mathrm{K}(\sqrt[p]{\mathrm{D}}) = \mathrm{E}(\zeta)$*.*

[The map $\mathrm{E} \mapsto \mathrm{D}$ defined by $\mathrm{E}(\zeta) = \mathrm{K}(\sqrt[p]{\mathrm{D}})$ gives a bijection between the degree-p cyclic extensions of F and $\mathbf{F}_p$-lines in $\varepsilon(\mathrm{K}^\times/\mathrm{K}^{\times p})$.]

Let us summarise. Let N be the maximal elementary abelian p-extension of F. The results of this § say that $\mathrm{NK} = \mathrm{K}(\sqrt[p]{\mathrm{V}})$, where $\mathrm{V} = \varepsilon(\mathrm{K}^\times/\mathrm{K}^{\times p})$ is the ω-eigenspace for the action of Δ on $\mathrm{K}^\times/\mathrm{K}^{\times p}$.

3. Notations. — The notation to be used in §4 has been collected here for reference, and will also be recalled as needed.

— $\mathrm{F}, \zeta, \mathrm{K}, \Delta, \omega, \varepsilon, \mathrm{V}$: F is a finite extension of $\mathbf{Q}_p$ which is regular in the sense of Shafarevich : $\zeta \notin \mathrm{F}$; so $p \neq 2$. Put $\mathrm{K} = \mathrm{F}(\zeta)$, and keep the notation $\Delta = \mathrm{Gal}(\mathrm{K}|\mathrm{F})$, $\omega : \Delta \to (\mathbf{Z}/p\mathbf{Z})^\times$, $\varepsilon \in \mathbf{F}_p[\Delta]$, $\mathrm{V} = \varepsilon(\mathrm{K}^\times/\mathrm{K}^{\times p})$ from §2.

— e, f, e_1 : e is the ramification index of $\mathrm{F}|\mathbf{Q}_p$, and f the residual degree. We put $e_1 = e/(p-1)$, which need not be an integer.

— m, s, r : s is the ramification index of K|F, and r the residual degree, so $m = sr$ equals $\mathrm{Card}\,\Delta = [\mathrm{K} : \mathrm{F}]$. In particular, r and s are prime to p. Notice that the ramification index of $\mathrm{K}|\mathbf{Q}_p$ is es and the residual degree fr. Also, $e_1 s$ is an integer because K contains ζ.

— k, q, F_r, k_r : k is the residue field of F, $q = p^f$ is its cardinality, F_r is the maximal unramified extension of F in K, and k_r is the common residue field of F_r and K. We have $[\mathrm{F}_r : \mathrm{F}] = r$, $[\mathrm{K} : \mathrm{F}_r] = s$.

Let us indicate how s and r can be computed. Adjoining $\zeta = \sqrt[p]{1}$ to F is the same as adjoining $\sqrt[p-1]{-p}$ [**2**, prop. 24], so that the degree $[\mathrm{K} : \mathrm{F}] = m$ equals the order of $\overline{-p} \in \mathrm{F}^\times/\mathrm{F}^{\times p-1}$; this order divides $p-1$. Momentarily let $s > 0$ be the smallest integer such that $\overline{-p}^s \in k^\times/k^{\times p-1}$; it is also the smallest integer such that $p-1 \,|\, es$. It is clear that the ramification index of K|F is s and the residual degree $r = m/s$. Indeed, if $u \in \mathrm{F}^\times$ is a unit such that $\bar{u} = \overline{-p}^s$, then the order of $\bar{u} \in k^\times/k^{\times p-1}$ is r, and K contains $\sqrt[p-1]{u}$, in the shape of $(\sqrt[p-1]{-p})^s$. On the one hand, the extension $\mathrm{F}_r = \mathrm{F}(\sqrt[p-1]{u})$ is unramified of degree r over F. On the other hand, the extension $\mathrm{K}|\mathrm{F}_r$ is totally ramified of degree s because $\overline{-p} \in \mathrm{F}_r^\times/\mathrm{F}_r^{\times p-1}$ has order s, and s is the smallest exponent (> 0) such that $\overline{-p}^s \in k_r^\times/k_r^{\times p-1}$.

— ϖ, π, v, w : ϖ is a uniformiser of F, π is the uniformiser $1-\zeta$ of $\mathbf{Q}_p(\zeta)$, v is the valuation on F such that $v(\varpi) = 1$ and w is the valuation on K such that $w(\varpi) = s$.

— $\mathfrak{o}, \mathfrak{O}, \mathfrak{p}, \mathfrak{P}, \mathrm{U}_i, \bar{\mathrm{U}}_i$: Let $\mathfrak{o}, \mathfrak{O}$ be the rings of integers of F, K and $\mathfrak{p}, \mathfrak{P}$ their unique maximal ideals. The $\mathbf{F}_p$-space $\bar{\mathrm{U}}_0 = \mathrm{K}^\times/\mathrm{K}^{\times p}$ comes with the filtration $(\bar{\mathrm{U}}_i)_{i>0}$, where $\mathrm{U}_i = 1 + \mathfrak{P}^i$; we also have $\overline{\mathfrak{O}^\times} = \bar{\mathrm{U}}_1$. We have $\bar{\mathrm{U}}_i = \{1\}$ for $i > pe_1 s$, and $\bar{\mathrm{U}}_{pe_1 s}$ is a line [**2**, prop. 42].

— $\mu, n, \xi, \bar{\mu}$: μ is the p^∞-torsion subgroup of $\mathfrak{O}^\times$; it is cyclic of order p^n, and ξ is a generator. We have $n > 0$ by hypothesis, but $n > 1$ is possible. (As an example, consider $\mathrm{F} = \mathbf{Q}_p(\xi)^\Delta$, where $\Delta = (\mathbf{Z}/p\mathbf{Z})^\times$ is identified as a subgroup of $\mathrm{Gal}(\mathbf{Q}_p(\xi)|\mathbf{Q}_p) = (\mathbf{Z}/p^m\mathbf{Z})^\times$ and ξ is a primitive p^m-th root of 1. As $[\mathrm{F} : \mathbf{Q}_p] = p^{m-1}$, it does not contain ζ, but $\mathrm{F}(\zeta) = \mathbf{Q}_p(\xi)$, so $n = m$). Finally, $\bar{\mu} \subset \bar{\mathrm{U}}_1$ is the image of μ; it is generated by $\bar{\xi}$.

— $a(i), b^{(i)}$: For every $i > 0$, put $a(i) = \left\lfloor \dfrac{i-1}{p-1} \right\rfloor$ and $b^{(i)} = i + a(i)$. Notice that $i \mapsto b^{(i)}$ is an increasing bijection of $\mathbf{N}^*$ with the set of integers in $\mathbf{N}^*$ prime to p.

— $\mathrm{N}, \mathrm{G}, \mathrm{H}$: N is the maximal elementary abelian p-extension of F, $\mathrm{G} = \mathrm{Gal}(\mathrm{N}|\mathrm{F})$, $\mathrm{H} = \mathrm{Gal}(\mathrm{NK}|\mathrm{K})$.

4. Regular local number fields. — Recall that lines in $\mathrm{V} \subset \mathrm{K}^\times/\mathrm{K}^{\times p}$ correspond to degree-p cyclic extensions of F. We would like to determine the filtration $\mathrm{V}_i = \mathrm{V} \cap \bar{\mathrm{U}}_i$ on V.

We shall go about it slowly, treating some special cases first in order to bring out the essential ideas. Almost the only thing we use is the fact that the unique ramification break of a degree-p cyclic extension of F occurs at -1 or at $b^{(i)}$ for some $i \in [1, e]$.

With the notation introduced in §2, it is clear that $\mathrm{V}_{pi} = \mathrm{V}_{pi+1}$ for every $i \neq e_1 s$ and that $\mathrm{V}_{pe_1 s+1} = \{\bar{1}\}$ [**2**, prop. 42]. Let us show first that $\mathrm{V} \subset \bar{\mathrm{U}}_1$ and that it contains the lines $\bar{\mu}, \bar{\mathrm{U}}_{pe_1 s}$.

Lemma 5. — *With these notations,* $\bar{\mathrm{U}}_{pe_1 s} \subset \mathrm{V} \subset \bar{\mathrm{U}}_1$ *and* $\bar{\mu} \subset \mathrm{V}$.

$\bar{\mu} \subset \mathrm{V}$: Let $\tau \in \Delta$ be a generator and let $g \in (\mathbf{Z}/p^n\mathbf{Z})^\times$ be such that $\tau(\xi) = \xi^g$; we have to show that $g \equiv \omega(\tau) \pmod{p}$. Now, $\zeta = \xi^{p^{n-1}}$ is a primitive p-th root of 1, so $\tau(\zeta) = \zeta^{\omega(\tau)} = \xi^{\omega(\tau)p^{n-1}}$, by hypothesis. But we also have $\tau(\zeta) = \tau(\xi)^{p^{n-1}} = \xi^{gp^{n-1}}$, so that $gp^{n-1} \equiv \omega(\tau)p^{n-1} \pmod{p^n}$, and hence $g \equiv \omega(\tau) \pmod{p}$.

$\mathrm{V} \subset \bar{\mathrm{U}}_1$: Let $w : \mathrm{K}^\times \to \mathbf{Z}$ be the surjective valuation, so that $\bar{x} \in \bar{\mathrm{U}}_1 \Leftrightarrow w(x) \in p\mathbf{Z}$ $(x \in \mathrm{K}^\times)$. Suppose that $\bar{x} \in \mathrm{V}$ for some $x \in \mathrm{K}^\times$, and let $\tau \in \Delta$ be a generator. By hypothesis, $\tau(x) = x^{\omega(\tau)}y^p$ for some $y \in \mathrm{K}^\times$. Taking valuations, we get $w(x) \equiv w(x)\omega(\tau) \pmod{p}$, and, as $\omega(\tau) \not\equiv 1 \pmod{p}$, we conclude that $w(x) \equiv 0 \pmod{p}$, and hence $\bar{x} \in \bar{\mathrm{U}}_1$.

$\bar{\mathrm{U}}_{pe_1s} \subset \mathrm{V}$: Let $\alpha \in \mathfrak{o}^\times$ be a unit of F the trace of whose reduction $\mathrm{S}_{k|\mathbf{F}_p}(\hat{\alpha}) \neq 0$ in $\mathbf{F}_p$. When α is considered as a unit of K, we have $\mathrm{S}_{k_r|\mathbf{F}_p}(\hat{\alpha}) = r\mathrm{S}_{k|\mathbf{F}_p}(\hat{\alpha})$, which is still $\neq 0$, for $r \not\equiv 0 \pmod{p}$. The line $\bar{\mathrm{U}}_{pe_1s}$ is therefore generated by the image of $1 + \alpha p\pi$, where $\pi = 1 - \zeta$; see the discussion after [**2**, prop. 33]. But for every $\tau \in \Delta$, we have $\tau(\pi) \equiv \omega(\tau)\pi \pmod{\pi^2}$, so

$$\tau(1 + \alpha p\pi) \equiv 1 + \omega(\tau)\alpha p\pi \equiv (1 + \alpha p\pi)^{\omega(\tau)} \pmod{\mathfrak{P}^{pe_1s+1}}$$

(recalling that $\pi\mathfrak{O} = \mathfrak{P}^{e_1s}$, $p\mathfrak{O} = \mathfrak{P}^{es}$, $e = (p-1)e_1$), which shows that $\tau(1 + \alpha p\pi) = (1 + \alpha p\pi)^{\omega(\tau)}\beta^p$ for some $\beta \in \mathrm{U}_1$, and hence $\overline{1 + \alpha p\pi} \in \mathrm{V}$.

Consider for a moment the special case $\mathrm{F} = \mathbf{Q}_p$, so that $e_1 = 1$ and $\pi = 1-\zeta$ is a uniformiser of K. It is easily seen that $\mathrm{V}_p = \mathrm{V}_{p-1} = \cdots = \mathrm{V}_2$: if $\bar{x} \in \mathrm{V}_i$ for some $i \in [2, p]$ and some $x \equiv 1 + \alpha\pi^j \pmod{\pi^{j+1}}$ ($\alpha \in \mathbf{Z}_p^\times$), then computing $\tau(\bar{x})$ in two different ways leads to the result.

Indeed, working $\pmod{\pi^{j+1}}$, we have $\tau(x) \equiv 1+\alpha\tau(\pi) \equiv 1+\alpha\omega(\tau)^j\pi^j$ on the one hand. On the other hand, as $\bar{x} \in \mathrm{V}$, we have $\tau(x) = x^{\omega(\tau)}y^p$ for some $y \in \mathrm{U}_1$. But $y^p \equiv 1$, so $\tau(x) \equiv (1 + \alpha\pi)^{\omega(\tau)} \equiv 1 + \omega(\tau)\alpha\pi$. The two computations imply $\omega(\tau)^{j-1} \equiv 1 \pmod{\pi}$, and in fact $\pmod{p}$, because $\omega(\tau) \in \mathbf{Z}_p^\times$. But $\omega(\tau)^{j-1} \equiv 1 \pmod{p}$ holds for a generator $\tau \in \Delta$ (which has order $p-1$) only when $j = p$. It follows that $\mathrm{V}_p = \mathrm{V}_2$ and hence $\mathrm{V} = \bar{\mathrm{U}}_p\bar{\mu}$ [**1**, p. 156]; the line $\bar{\mathrm{U}}_p$ corresponds to the unramified degree-p extension, and the line $\bar{\mu}$ to the cyclotomic $(\mathbf{Z}/p\mathbf{Z})$-extension.

The result $\mathrm{V}_2 = \bar{\mathrm{U}}_p$ (when $\mathrm{F} = \mathbf{Q}_p$) could also have been obtained by remarking that in this case the unique ramification break of a ramified degree-p cyclic extension L|K coming from F occurs at $p-1$ [**2**, prop. 63], an argument which works for any finite extension $\mathrm{F}|\mathbf{Q}_p$ (such that $\zeta \notin \mathrm{F}$). Hence the following bit of information about the filtration on V :

Lemma 6. — *We have* $\bar{\mathrm{U}}_{pe_1s} = \mathrm{V}_{pe_1s-1} = \cdots = \mathrm{V}_{pe_1s-s+1}$, *where* s *is the ramification index of* K|F.

Let $\mathrm{D} \subset \mathrm{V}_{pe_1s-s+1}$ be a line such that $\mathrm{D} \neq \bar{\mathrm{U}}_{pe_1s}$, E|F the corresponding degree-p cyclic extension, and $t > 0$ its unique ramification break. The unique ramification break of $\mathrm{E}(\zeta)|\mathrm{K}$ occurs at ts [**2**, proof of prop. 63] on the one hand, and at $s-i$ for some $i \in [1, s[$, on the other [**2**, prop. 60]. But $ts = s-i$ is impossible, so there is no such D, and hence $\bar{\mathrm{U}}_{pe_1s} = \mathrm{V}_{pe_1s-s+1}$.

Let us next determine the $\mathbf{F}_p$-dimension of $\mathrm{V}_{pe_1s-s}/\mathrm{V}_{pe_1s-s+1}$.

Lemma 7. — *We have* $\dim_{\mathbf{F}_p} \mathrm{V}_{pe_1s-s}/\mathrm{V}_{pe_1s-s+1} = f$, *where* $f = [k : \mathbf{F}_p]$ *is the residual degree of* $\mathrm{F}|\mathbf{Q}_p$.

Let ϖ be a uniformiser of F and recall that $\pi = 1 - \zeta$, where $\zeta \in \mathrm{K}$ is a primitive p-th root of 1. We have $w(p\pi\varpi^{-1}) = pe_1 s - s$, so that $p\pi\varpi^{-1}$ is an $\mathfrak{O}$-basis of $\mathfrak{P}^{pe_1 s - s}$.

Use this basis to identify $\bar{\mathrm{U}}_{pe_1 s-s}/\bar{\mathrm{U}}_{pe_1 s-s+1}$ with $k_r = \mathfrak{O}/\mathfrak{P}$, the residue field of K, by sending $\overline{1 + \alpha p\pi\varpi^{-1}}$ ($\alpha \in \mathfrak{O}$) to $\hat{\alpha}$. We claim that then $\mathrm{V}_{pe_1 s-s}/\mathrm{V}_{pe_1 s-s+1}$ gets identified with the subspace $k \subset k_r$. The idea is to show that the $\mathbf{F}_p[\Delta]$-module structure on k_r coming from the said identification is the usual structure twisted by ω.

Let $\tau \in \Delta$ be a generator. Recall that $\tau(\pi) \equiv \omega(\tau)\pi \pmod{\pi^2}$ and that $\tau(\alpha) \equiv \alpha^q \pmod{\varpi}$ for every integer $\alpha \in \mathrm{F}_r$, where $q = \operatorname{Card} k$ is the residual cardinality of F. Because $pe_1 s - s$ is prime to p, the group $\bar{\mathrm{U}}_{pe_1 s-s}/\bar{\mathrm{U}}_{pe_1 s-s+1}$ is canonically isomorphic to $\mathrm{U}_{pe_1 s-s}/\mathrm{U}_{pe_1 s-s+1}$ [**2**, proof of prop. 42] and because K and F_r have the same residue field, every element of $\mathrm{U}_{pe_1 s-s}/\mathrm{U}_{pe_1 s-s+1}$ is represented by $1 + \alpha p\pi\varpi^{-1}$ for some integer $\alpha \in \mathrm{F}_r$.

Now, $\tau(\alpha p\pi\varpi^{-1}) \equiv \omega(\tau)\alpha^q p\pi\varpi^{-1} \pmod{\mathfrak{P}^{pe_1 s-s+1}}$, from which it follows that $\tau(\hat{\alpha}) = \omega(\tau)\hat{\alpha}^q$ for every $\hat{\alpha} \in k_r$. The ω-eigenspace for this new Δ-action on k_r is thus k, the set of $\hat{\alpha} \in k_r$ such that $\hat{\alpha}^q = \hat{\alpha}$.

But $\mathrm{V}_{pe_1 s-s}/\mathrm{V}_{pe_1 s-s+1} \subset \bar{\mathrm{U}}_{pe_1 s-s}/\bar{\mathrm{U}}_{pe_1 s-s+1}$ is the ω-eigenspace, hence it gets identified with $k \subset k_r$, proving the lemma.

We shall need the following elementary fact.

Lemma 8. — *The number of prime-to-p integers in $[1, pe_1[$ is e, and they are*

$$1 = b^{(1)} < b^{(2)} < \cdots < b^{(e)} \qquad (< pe_1),$$

where $b^{(i)} = i + a(i)$ and $a(i) = \left\lfloor \dfrac{i-1}{p-1} \right\rfloor$ for every integer $i \in [1, e]$.

Write $e = (p-1)c + c'$, with $c \in \mathbf{N}$ and the remainder $c' \in [0, p-1[$, so that $e_1 = c + c'/(p-1)$, where $c'/(p-1) \in [0, 1[$ is rational, and

$$pe_1 = pc + \frac{pc'}{p-1} = pc + c' + \frac{c'}{p-1}.$$

It is now clear that the number of integers in $[1, pe_1[$ which are prime to p is $pc + c' - c = e$. That they are precisely $b^{(1)}, \ldots, b^{(e)}$ is left as an exercise.

Recall that the unique ramification break of a ramified degree-p cyclic extension L|F occurs at $b^{(i)}$ for some $i \in [1, e]$; see for example [**2**, prop. 63].

Lemma 9. — *For $i \in [1, e]$, we have $\dim_{\mathbf{F}_p} \mathrm{V}_{pe_1 s - sb^{(i)}}/\mathrm{V}_{pe_1 s - sb^{(i)}+1} = f$, and $\mathrm{V}_{pe_1 s - b^{(i-1)} s} = \mathrm{V}_{pe_1 s - b^{(i)} s + 1}$ (with the convention $b^{(0)} = 0$).*

We have already seen the case $i = 1$ of the first part in lemma 7, whose proof can be adapted to the case $i > 1$ by using the $\mathfrak{O}$-basis $p\pi\varpi^{-b^{(i)}}$ of $\mathfrak{P}^{pe_1s-b^{(i)}s}$ to identify $\bar{\mathrm{U}}_{pe_1s-b^{(i)}s}/\bar{\mathrm{U}}_{pe_1s-b^{(i)}s+1}$ with $k_r(1)$, the Δ-module k_r with the action twisted by ω.

The case $i = 1$ of the second part is lemma 6, and the same proof works for $i > 1$. Indeed, let $\mathrm{D} \subset \mathrm{V}_{pe_1s-b^{(i)}s+1}$ be an $\mathbf{F}_p$-line and suppose that the unique ramification break of the corresponding degree-p cyclic extension E|F occurs at some $t < b^{(i)}$. As t is prime to p, we have $t \leq b^{(i-1)}$, and it follows that $\mathrm{D} \subset \mathrm{V}_{pe_1s-b^{(i-1)}s}$.

Lemma 10. — *We have* $\mathrm{V}_{pe_1s-b^{(e)}s} = \mathrm{V}$. *Equivalently,* $\mathrm{V} \subset \bar{\mathrm{U}}_{pe_1s-b^{(e)}s}$.

The idea of the proof is the same as for the last few lemmas. Explicitly, let $\mathrm{D} \subset \mathrm{V}$ be an $\mathbf{F}_p$-line, E|F the corresponding degree-p cyclic extension, and t the unique ramification break of $\mathrm{Gal}(\mathrm{E}|\mathrm{F})$; we have $t \leq b^{(e)}$. The unique ramification break of $\mathrm{Gal}(\mathrm{E}(\zeta)|\mathrm{K})$ occurs at $ts \leq b^{(e)}s$, hence $\mathrm{D} \subset \mathrm{V}_{pe_1s-b^{(e)}s}$.

(We know that $\bar{\mu} \subset \mathrm{V}$ (lemma 5), so lemma 9 leads to the unexpected consequence that $\bar{\mu} \subset \bar{\mathrm{U}}_{pe_1s-b^{(e)}s}$.)

Let us pause for a moment to summarise what we have learnt about the filtration on V. Let us agree to write $\mathrm{B} \subset_c \mathrm{A}$ if A is an $\mathbf{F}_p$-space and B is a subspace of A of codimension c. The filtration on V begins with

$$\{1\} \subset_1 \mathrm{V}_{pe_1s} = \mathrm{V}_{pe_1s-s+1} \subset_f \mathrm{V}_{pe_1s-s}$$

and continues, for every integer $i \in [1, e[$, with

$$\mathrm{V}_{pe_1s-b^{(i)}s} = \mathrm{V}_{pe_1s-b^{(i+1)}s+1} \subset_f \mathrm{V}_{pe_1s-b^{(i+1)}s},$$

to end finally with $\mathrm{V}_{pe_1s-b^{(e)}s} = \mathrm{V}$. It follows that the $\mathbf{F}_p$-dimension of V is $1 + ef = 1 + [\mathrm{F} : \mathbf{Q}_p]$. In short, the breaks in the filtration $(\mathrm{V}_j)_{j>0}$ occur at $j = pe_1s$, where the order of the group drops by a factor of p, and at $j = pe_1s - b^{(i)}s$ for every integer $i \in [1, e]$, where the order drops by a factor of $q = p^f$.

Now let N be the maximal elementary abelian p-extension of F, so that $\mathrm{NK} = \mathrm{K}(\sqrt[p]{\mathrm{V}})$ (lemma 4). Let us briefly indicate how to compute the ramification filtration on $\mathrm{G} = \mathrm{Gal}(\mathrm{N}|\mathrm{F})$ using the preceding results, without any appeal to local class field theory.

In view of the the two cases treated earlier (finite extensions of $\mathbf{Q}_p$ having a primitive p-th root of 1 [**2**], local function fields [**3**]), it is natural to look for an "orthogonality relation" for the pairing

$$\mathrm{G} \times \mathrm{V} \to {}_p\mu$$

which sends $(\sigma, \bar{x})$ to $\sigma(\sqrt[p]{x})/\sqrt[p]{x}$, after having made the identification $\mathrm{G} \to \mathrm{H}$, where $\mathrm{H} = \mathrm{Gal}(\mathrm{NK}|\mathrm{K})$. This is the content of the prop. 11.

For a subspace $\mathrm{E} \subset \mathrm{G}$, denote by $\mathrm{E}^\perp \subset \mathrm{V}$ the subspace such that $\mathrm{N}^\mathrm{E}\mathrm{K} = \mathrm{K}(\sqrt[p]{\mathrm{E}^\perp})$. For example, if $\mathrm{T} \subset \mathrm{G}$ is the inertia subgroup (so that N^T is the degree-p unramified extension of F), then $\mathrm{T}^\perp = \mathrm{V}_{pe_1s}$. If we identify G with H to get a pairing $\mathrm{G} \times \mathrm{V} \to {}_p\mu$, then $\mathrm{E}^\perp$ is the orthogonal of E. Denote by $\mathrm{D}^\perp \subset \mathrm{G}$ the orthogonal of a subspace $\mathrm{D} \subset \mathrm{V}$.

Proposition 11. — *We have* $\mathrm{G}^u = \mathrm{G}^1$ *for* $u \in \,]-1, 1]$, $\mathrm{G}^u = \{1\}$ *for* $u > b^{(e)}$, *and*

$$(\mathrm{G}^u)^\perp = \mathrm{V}_{pe_1s - \lceil u \rceil s + 1} \qquad (u \in [1, b^{(e)}])$$

under $\mathrm{G} \times \mathrm{V} \to {}_p\mu$, *the pairing coming from the identification* $\mathrm{G} \to \mathrm{H}$.

Notice first that $\mathrm{G}^u \neq \mathrm{G}$ for $u > -1$, because the quotient $\mathrm{Gal}(\mathrm{F}_p|\mathrm{F})$ of G has its break at -1, where F_p is the unramified degree-p extension of F. It follows that the index of $\mathrm{G}^u \subset \mathrm{G}^{-1}$ is > 1 for $u > -1$.

Let $u \in \,]-1, 1]$ and let E be a hyperplane containing G^u, so that G/E is cyclic of order p. As the filtration on G/E is the quotient of the filtration on G, the ramification break of G/E occurs somewhere $< u$ (because $\mathrm{G}^u \subset \mathrm{E}$). But the only degree-$p$ cyclic extension of F whose ramification break is < 1 is the unramified one. So $\mathrm{E} = \mathrm{V}_{pe_1s}^\perp$ is the only hyperplane containing G^u. This implies that $\mathrm{G}^u = \mathrm{E} = \mathrm{G}^1 = \mathrm{V}_{pe_1s}^\perp$.

Suppose next that $u > b^{(e)}$; it suffices to show that every hyperplane $\mathrm{E} \subset \mathrm{G}$ contains G^u. Now $\mathrm{G}^u \subset \mathrm{E}$ if and only if the unique ramification break of G/E occurs somewhere $< u$. But this is true for every E, because $u > b^{(e)}$. Hence $\mathrm{G}^u = \{1\}$.

It remains to determine $\mathrm{G}^{u\perp}$ for $u \in [1, b^{(e)}]$. Take a line $\mathrm{D} \neq \mathrm{V}_{pe_1s}$ in V and denote by $t \neq -1$ be the unique ramification break of $\mathrm{G}/\mathrm{D}^\perp$, so that the unique ramification break of $\mathrm{K}(\sqrt[p]{\mathrm{D}})|\mathrm{K}$ occurs at ts. Then

$$\mathrm{D} \subset \mathrm{G}^{u\perp} \Leftrightarrow (\mathrm{G}/\mathrm{D}^\perp)^u = 0 \Leftrightarrow t < u \Leftrightarrow ts < \lceil u \rceil s \Leftrightarrow \mathrm{D} \subset \mathrm{V}_{pe_1s - \lceil u \rceil s + 1}.$$

As the two subspaces $\mathrm{G}^{u\perp}$ and $\mathrm{V}_{pe_1s - \lceil u \rceil s + 1}$ of V contain the same lines, they are equal. Note in particular that $\mathrm{G}^{b^{(e)}\perp} = \mathrm{V}_{pe_1s - b^{(e-1)}s}$ (lemma 9), which has codimension f in V (lemma 10).

Now it is an easy matter to determine the filtration on G, knowing as we do the filtration on V.

Corollary 12. — *The upper ramification breaks of* $(\mathrm{G}^u)_{u\in[-1,+\infty[}$ *occur at* -1 *and at the* $b^{(i)}$ *for* $i \in [1,e]$ *; the codimensions are given by*

$$\{1\} \subset_f \mathrm{G}^{b^{(e)}} \subset_f \cdots \subset_f \mathrm{G}^{b^{(2)}} \subset_f \mathrm{G}^{b^{(1)}} = \mathrm{G}^0 \subset_1 \mathrm{G}^{-1} = \mathrm{G},$$

where $\subset_f$ *means "codimension* f*". In particular,* $\mathrm{G}^{pj} = \mathrm{G}^{pj+1}$ *for every* j*.*

This follows from prop. 11 and our knowledge of the filtration on V (lemmas 5–10).

It is also an easy matter to determine the filtration in the lower numbering on G. We have the following table for the index of G^u in G^0 for $u \in [0,+\infty[$:

$u \in$	$[0,b^{(1)}]$	$]b^{(1)},b^{(2)}]$	$\cdots$	$]b^{(e-1)},b^{(e)}]$	$]b^{(e)},+\infty[$
$(\mathrm{G}^0 : \mathrm{G}^u) =$	1	q	$\cdots$	q^{e-1}	q^e

The e positive ramification breaks in the lower numbering occur therefore at $b_{(i)} = \psi_{\mathrm{N|F}}(b^{(i)})$ [**7**, p. 74] for $i \in [1,e]$. As in [**3**], we have

$$b_{(i)} = (1 + q + \cdots + q^{i-1}) + (q^{p-1} + \cdots + q^{a(i)(p-1)}).$$

Corollary 13. — *The lower ramification breaks of* $(\mathrm{G}_l)_{l\in[-1,+\infty[}$ *occur at* -1 *and at the* $b_{(i)}$ *for* $i \in [1,e]$ *; the codimensions are given by*

$$\{1\} \subset_f \mathrm{G}_{b_{(e)}} \subset_f \cdots \subset_f \mathrm{G}_{b_{(2)}} \subset_f \mathrm{G}_{b_{(1)}} \subset_1 \mathrm{G}_{-1} = \mathrm{G}.$$

An application of [**3**, lemma 2] now gives the exponent $v_{\mathrm{N}}(\mathfrak{D}_{\mathrm{N|F}})$ of the different $\mathfrak{D}_{\mathrm{N|F}}$ as

$$v_{\mathrm{N}}(\mathfrak{D}_{\mathrm{N|F}}) = (1 + b^{(e)})q^e - (1 + b_{(e)})$$

and the exponent $v(d_{\mathrm{N|F}})$ of the discriminant as $v(d_{\mathrm{N|F}}) = p.v_{\mathrm{N}}(\mathfrak{D}_{\mathrm{N|F}})$, because the residual degree of N|F is p.

Local class field theory was needed in [**3**, after prop. 5] to compute the filtration on G and thereby obtain these values for the exponent of the different and the discriminant.

5. Overall summary. — Let p be a prime number, K a finite extension of $\mathbf{Q}_p$ or of $\mathbf{F}_p(\!(\pi)\!)$, M the maximal elementary abelian p-extension of K, and $\mathrm{G} = \mathrm{Gal}(\mathrm{M|K})$. We have seen that it is possible to determine the filtration (in the upper numbering) on G using only Kummer theory in the local number field case, and only Artin-Schreier theory in the local function field case. In the former case — where G is finite — the lower numbering can also be determined. In the latter case, one can determine the lower numbering on the finite quotients of G.

Consider first a finite extension $\mathrm{K}|\mathbf{Q}_p$ (of ramification index e and residual degree f) containing a primitive p-root ζ of 1. The filtration on $\overline{\mathrm{K}^\times} = \mathrm{K}^\times/\mathrm{K}^{\times p}$ is easily determined and looks like

$$\{1\} \subset_1 \bar{\mathrm{U}}_{pe_1} \subset_f \bar{\mathrm{U}}_{b^{(e)}} \subset_f \cdots \subset_f \bar{\mathrm{U}}_{b^{(1)}} \subset_1 \bar{\mathrm{U}}_0 = \overline{\mathrm{K}^\times},$$

where $e_1 = e/(p-1)$ [**2**, prop. 42]. If a line $\mathrm{D} \subset \overline{\mathrm{K}^\times}$ is in $\bar{\mathrm{U}}_m$ but not in $\bar{\mathrm{U}}_{m+1}$ (which forces $m = 0$ or $m = b^{(i)}$ for some $i \in [1, e]$ or $m = pe_1$), then the unique ramification break of $\mathrm{K}(\sqrt[p]{\mathrm{D}})$ occurs at $pe_1 - m$ if $m \neq pe_1$ [**2**, prop. 60], at -1 if $m = pe_1$ [**2**, prop. 16]. The filtration $(\mathrm{G}^u)_u$ is completely determined by $\mathrm{G}^u = \mathrm{G}^1$ for $u \in \,]-1, 1]$, $\mathrm{G}^u = \{1\}$ for $u > pe_1$ and the orthogonality relation

$$(\mathrm{G}^u)^\perp = \bar{\mathrm{U}}_{pe_1 - \lceil u \rceil + 1}$$

for $u \in [1, pe_1]$ [**2**, Part IX], under the Kummer pairing $\mathrm{G} \times \overline{\mathrm{K}^\times} \to {}_p\mu$. This leads to the description

$$\{1\} \subset_1 \mathrm{G}^{pe_1} \subset_f \mathrm{G}^{b^{(e)}} \subset_f \cdots \subset_f \mathrm{G}^{b^{(2)}} \subset_f \mathrm{G}^{b^{(1)}} \subset_1 \mathrm{G}.$$

The ramification breaks in the lower numbering occur at -1, at the $b_{(i)}$ for $i \in [1, e]$, and at $b_{(e)} + q^e$, where $q = p^f$ [**3**, prop. 3].

Consider next a finite extension $\mathrm{K}|\mathbf{F}_p(\!(\pi)\!)$ (of residual degree f). The filtration on $\overline{\mathrm{K}} = \mathrm{K}/\wp(\mathrm{K})$ looks like

$$\{0\} \subset_1 \overline{\mathfrak{o}} \subset_f \overline{\mathfrak{p}^{-b^{(1)}}} \subset_f \overline{\mathfrak{p}^{-b^{(2)}}} \subset_f \cdots \subset \overline{\mathrm{K}}$$

[**3**], §6. If a line $\mathrm{D} \subset \overline{\mathrm{K}}$ is in $\overline{\mathfrak{p}^{-m}}$ but not in $\overline{\mathfrak{p}^{-m+1}}$ (which forces $m = 0$ or $m = b^{(i)}$ for some $i \in \mathbf{N}^*$), then the unique ramification break of $\mathrm{K}(\wp^{-1}(\mathrm{D}))$ occurs at m if $m \neq 0$ [**3**, prop. 14], at -1 if $m = 0$ [**3**, prop. 12]. The filtration $(\mathrm{G}^u)_u$ is completely determined by $\mathrm{G}^u = \mathrm{G}^1$ for $u \in \,]-1, 1]$ and the orthogonality relation

$$(\mathrm{G}^u)^\perp = \overline{\mathfrak{p}^{-\lceil u \rceil + 1}}$$

for $u > 0$ [**3**, prop. 17], under the Artin-Schreier pairing $\mathrm{G} \times \overline{\mathrm{K}} \to \mathbf{F}_p$, leading to the description

$$\{1\} \subset \cdots \subset_f \mathrm{G}^{b^{(2)}} \subset_f \mathrm{G}^{b^{(1)}} \subset_1 \mathrm{G}.$$

For $m \in \mathbf{N}$, the breaks in the lower numbering on $\mathrm{K}(\wp^{-1}(\mathfrak{p}^{-m}))$ occur at -1 and at $b_{(i)}$ for $i \in [1, c(m)]$, where $c(m) = m - \lfloor m/p \rfloor$ [**3**, prop. 19].

Consider lastly a finite extension $\mathrm{K}|\mathbf{Q}_p$ (of ramification index e and residual degree f) *not* containing ζ, such as the F in §3–4, and put $\mathrm{L} = \mathrm{K}(\zeta)$. We have determined the filtered subspace $\mathrm{V} \subset \overline{\mathrm{L}^\times}$ (§2, §4) lines D in which correspond to degree-p cyclic extensions E of K by the rule $\mathrm{L}(\sqrt[p]{\mathrm{D}}) = \mathrm{E}(\zeta)$. Lines in V correspond therefore to hyperplanes in G and lead to an orthogonality relation (prop. 11) which determines $(\mathrm{G}^u)_u$ (cor. 12) and $(\mathrm{G}_l)_l$ (cor. 13).

The information carried by V can be succintly expressed by posing $\mathrm{W}_i = \mathrm{V}_{pe_1 s - b^{(i)} s}$ for $i \in [0, e]$, where $e_1 = e/(p-1)$, s is the ramification index of L|K, and $b^{(0)} = 0$ by convention. We then have the picture

$$\{1\} \subset_1 \mathrm{W}_0 \subset_f \mathrm{W}_1 \subset_f \cdots \subset_f \mathrm{W}_e = \mathrm{V};$$

the line W_0 corresponds to the unramified degree-p extension of K, and, for every $i \in [1, e]$ and every line $\mathrm{D} \subset \mathrm{W}_i$ such that $\mathrm{D} \not\subset \mathrm{W}_{i-1}$, the unique ramification break of the corresponding degree-p cyclic extension E|K occurs at $b^{(i)}$. In particular, $v_{\mathrm{K}}(d_{\mathrm{E}|\mathrm{K}}) = (p-1)(1 + b^{(i)})$.

6. The contribution of cyclic extensions. — Let p be a prime number, $k|\mathbf{F}_p$ a finite extension, $q = p^f = \operatorname{Card} k$, and let F be a local field with residue field k. The preceding considerations can be applied to computing the contribution of cylic extensions to Serre's degree-p "mass formula" [**8**].

Recall that the formula in question asserts that $\sum_{\mathrm{L}} q^{-c(\mathrm{L})} = n$, where L runs through totally ramified extensions of F (in a fixed separable closure) of degree $n = [\mathrm{L} : \mathrm{F}]$, and $c(\mathrm{L}) = v_{\mathrm{F}}(d_{\mathrm{L}|\mathrm{F}}) - (n-1)$. One may ask for the contribution of *cyclic* extensions to this formula; the foregoing summary (§5) makes it possible to compute it.

[In the case $p = 2$, every separable quadratic extension is cyclic, so the contribution should be 100%; this has been verified in the characteristic-0 case [**2**, lemma 67]. We shall see that in the characteristic-2 case it amounts to the identity

$$\frac{2 + 2^2 + \cdots + 2^f}{2^{(2-1)f}} + \cdots + \frac{2^{(i-1)f+1} + 2^{(i-1)f+2} + \cdots + 2^{if}}{2^{(2i-1)f}} + \cdots = 2.]$$

Consider first the characteristic-p case.

Proposition 14. — *Let* $\mathrm{F} = k(\!(\pi)\!)$. *When* L *runs through ramified cyclic extensions of* F *of degree* p, *we have*

$$\sum_{\mathrm{L}} q^{-c(\mathrm{L})} = \frac{p}{q} \cdot \frac{q-1}{p-1} \cdot \sum_{i>0} q^{i-(p-1)b^{(i)}}, \tag{1}$$

where $b^{(i)} = i + a(i)$ *and* $a(i) = \lfloor (i-1)/(p-1) \rfloor$ *for every integer* $i > 0$.

The idea of the proof is clear from §5. Each (ramified, degree-p, cyclic) extension L|F has a unique ramification break, which equals $b^{(i)}$ for some $i > 0$; if so, then $c(\mathrm{L}) = (p-1)b^{(i)}$. These L correspond to $\mathbf{F}_p$-lines $\mathrm{D} \subset \overline{\mathfrak{p}^{-b^{(i)}}}$ such that $\mathrm{D} \not\subset \overline{\mathfrak{p}^{-b^{(i-1)}}}$. As the dimension of $\overline{\mathfrak{p}^{-b^{(i)}}}$ is $1+if$, the number of such lines D is $pq^{i-1}+p^2q^{i-1}+\cdots+p^fq^{i-1} = pq^{i-1}(q-1)/(p-1)$. So the contribution of such L (or such D) to the sum is

$$\frac{pq^{i-1}(q-1)}{(p-1)q^{(p-1)b^{(i)}}} = \frac{p}{q} \cdot \frac{q-1}{p-1} \cdot q^{i-(p-1)b^{(i)}},$$

and summing over all $i > 0$ gives the result. Note that, when $p = 2$, $i - (p-1)b^{(i)} = i - b^{(i)} = -a(i) = 1 - i$, so $\sum_{i>0} q^{i-(p-1)b^{(i)}} = q/(q-1)$.

Consider next the characteristic-0 case of a finite extension $\mathrm{F}|\mathbf{Q}_p$ with ramification index e and residual degree f; put $e_1 = e/(p-1)$ and $q = p^f$.

Proposition 15. — *Suppose that* $\mathrm{F}|\mathbf{Q}_p$ *contains a primitive* p*-th root of* 1. *When* L *runs through ramified degree-*p *cyclic extensions of* F*, we have*

$$\sum_{\mathrm{L}} q^{-c(\mathrm{L})} = \frac{p}{q^{(p-1)e}} + \frac{p}{q}\frac{q-1}{p-1} \sum_{i \in [1,e]} q^{i-(p-1)b^{(i)}}. \tag{2}$$

Ramified cyclic degree-p extensions L|F are of two kinds. If the unique ramification break t of $\mathrm{Gal}(\mathrm{L}|\mathrm{F})$ is prime to p, then $t = b^{(i)}$ for some $i \in [1, e]$; they are called *peu ramifiées*, correspond to lines in the $\mathbf{F}_p$-space $\bar{\mathrm{U}}_1$ other than the line $\bar{\mathrm{U}}_{pe_1}$, and contribute the second term on the right in (2), as we saw in the characteristic-p case (prop. 14).

If, on the other hand, $p|t$, then $t = pe_1$; such extensions L|K are called *très ramifiées* and correspond to $\mathbf{F}_p$-lines $\mathrm{D} \subset \mathrm{K}^\times/\mathrm{K}^{\times p}$ not contained in $\bar{\mathrm{U}}_1$. The number of such lines is pq^e. As we then have $c(\mathrm{L}) = pe$, this explains the presence of the first term on the right in (2).

Consider finally the characteristic-0 case in the absence of $\sqrt[p]{1}$.

Proposition 16. — *Suppose that* $\mathrm{F}|\mathbf{Q}_p$ *does not contain a primitive* p*-th root of* 1. *When* L *runs through ramified degree-*p *cyclic extensions of* F*,*

$$\sum_{\mathrm{L}} q^{-c(\mathrm{L})} = \frac{p}{q}\frac{q-1}{p-1} \sum_{i \in [1,e]} q^{i-(p-1)b^{(i)}}. \tag{3}$$

This follows easily from the last paragraph of §5 and the proof in the previous case. The only difference is that F now has no *très ramifiées*

extensions, which explains the absence in (3) of the first term on the right in (2). So, in the characteristic-0 case, a lesser proportion of degree-p extensions is cylic if $\sqrt[p]{1} \notin \mathrm{K}$ than if $\sqrt[p]{1} \in \mathrm{K}$, all other things being equal.

Remark. — Notice that the method allows us to compute the average $c(\mathrm{L})$ as L runs through ramified degree-p cyclic extensions of F of some given kind. We illustrate this with the case $\mathrm{F} = \mathbf{Q}_p(\sqrt[p]{1})$. For every $i \in [1, p]$, there are p^i extensions L such that $c(\mathrm{L}) = (p-1)i$, so the average is

$$\frac{\sum_{i\in[1,p]}(p-1)ip^i}{\sum_{i\in[1,p]}p^i} = \frac{p^{p+2} - p^{p+1} - p^p + 1}{p^p - 1}.$$

If we want L to be *peu ramifié*, the sums extend only over $i \in [1, p[$.

***

Bibliographic References

[**1**] Cassels (J). — *Local fields,* Cambridge University Press, Cambridge, 1986. xiv+360 pp.

[**2**] Dalawat (C). — *Local discriminants, kummerian extensions, and elliptic curves,* Journal of the Ramanujan Mathematical Society, **25** (2010) 1, pp. 25–80. Cf. arXiv:0711.3878.

[**3**] Dalawat (C). — *Further remarks on local discriminants,* 0909.2541.

[**4**] Dalawat (C). — *Serre's "formule de masse" in prime degree,* 1005.2016.

[**5**] Del Corso (I) and Dvornicich (R). — *The compositum of wild extensions of local fields of prime degree,* Monatsh. Math. **150** (2007) 4, pp. 271–288.

[**6**] Neumann (O). — *Two proofs of the Kronecker-Weber theorem "according to Kronecker, and Weber",* J. Reine Angew. Math. **323** (1981), 105–126.

[**7**] Serre (J-P). — *Corps locaux,* Publications de l'Université de Nancago, No. viii, Hermann, Paris, 1968, 245 pp.

[**8**] Serre (J-P). — *Une "formule de masse" pour les extensions totalement ramifiées de degré donné d'un corps local,* Comptes Rendus **286** (1978), pp. 1031–1036.